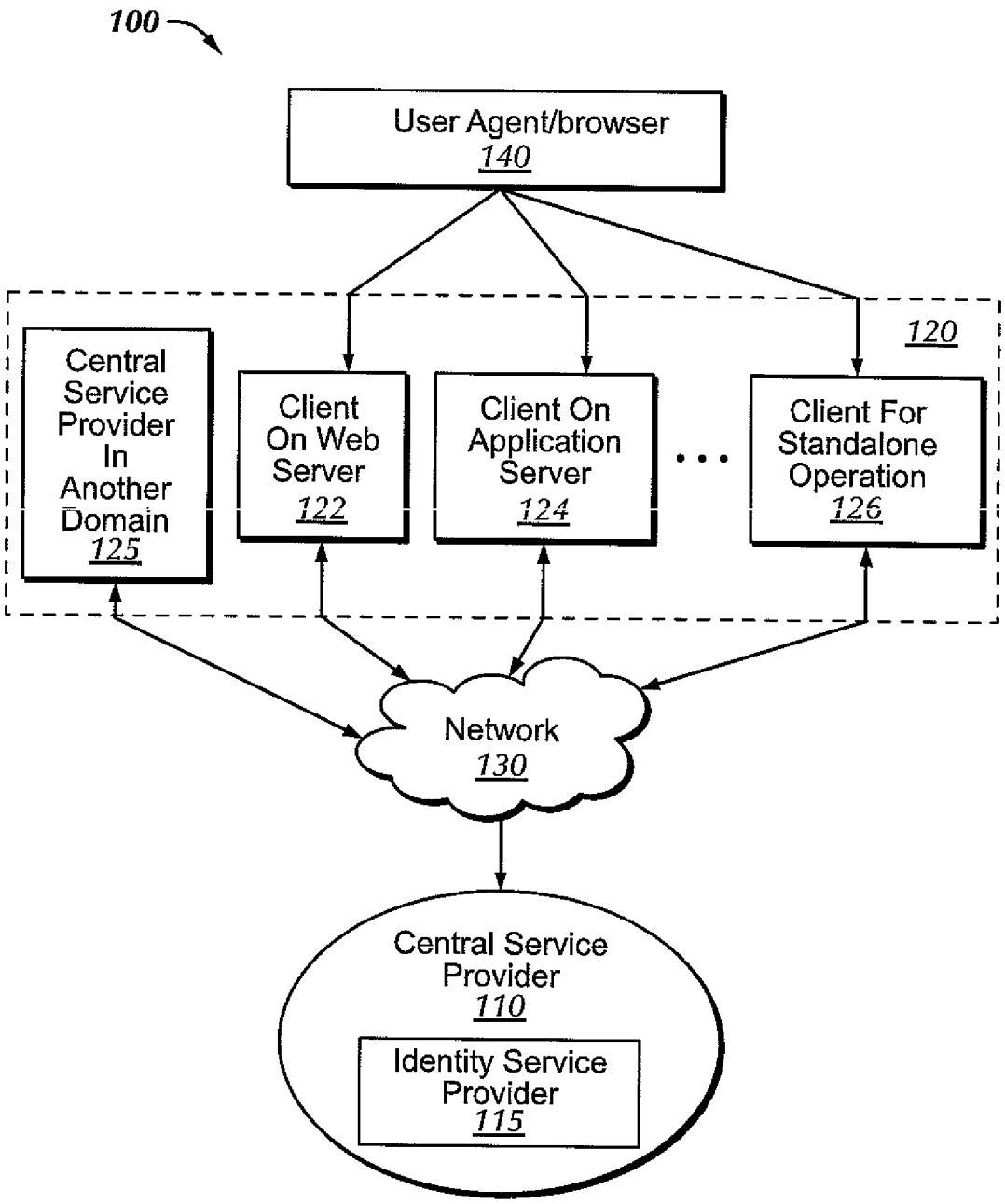
100
User Agent/browser
140
120
Central Service Provider In Another Domain
125
Client On Web Server
122
Client On Application Server
124
Client For Standalone Operation
126
Network
130
Central Service Provider
110
Identity Service Provider
115

FIG. 1

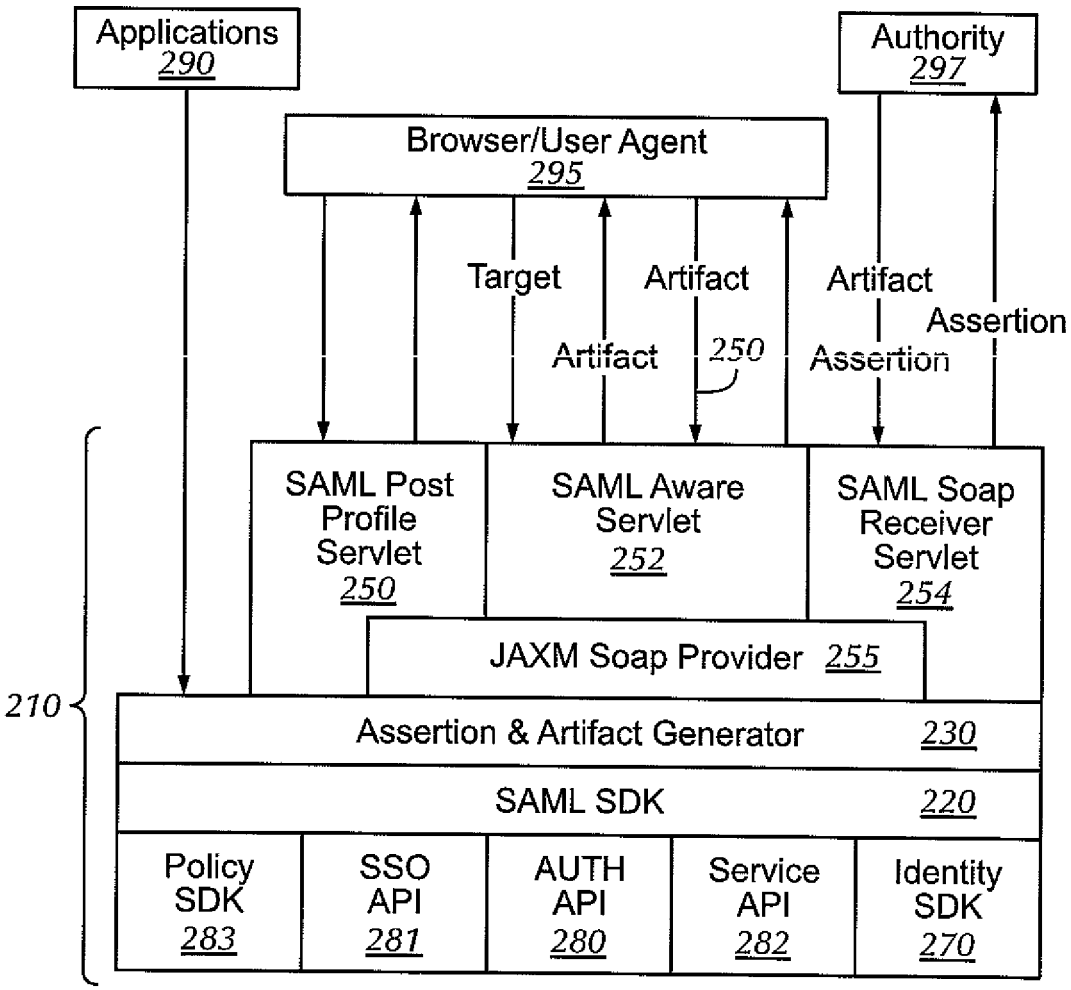
Applications
290
Authority
297
Browser/User Agent
295
Target
Artifact
Artifact
Assertion
Artifact
250
Assertion
SAML Post Profile Servlet
250
SAML Aware Servlet
252
SAML Soap Receiver Servlet
254
JAXM Soap Provider 255
210
Assertion & Artifact Generator 230
SAML SDK 220
Policy SDK
283
SSO API
281
AUTH API
280
Service API
282
Identity SDK
270

FIG. 2

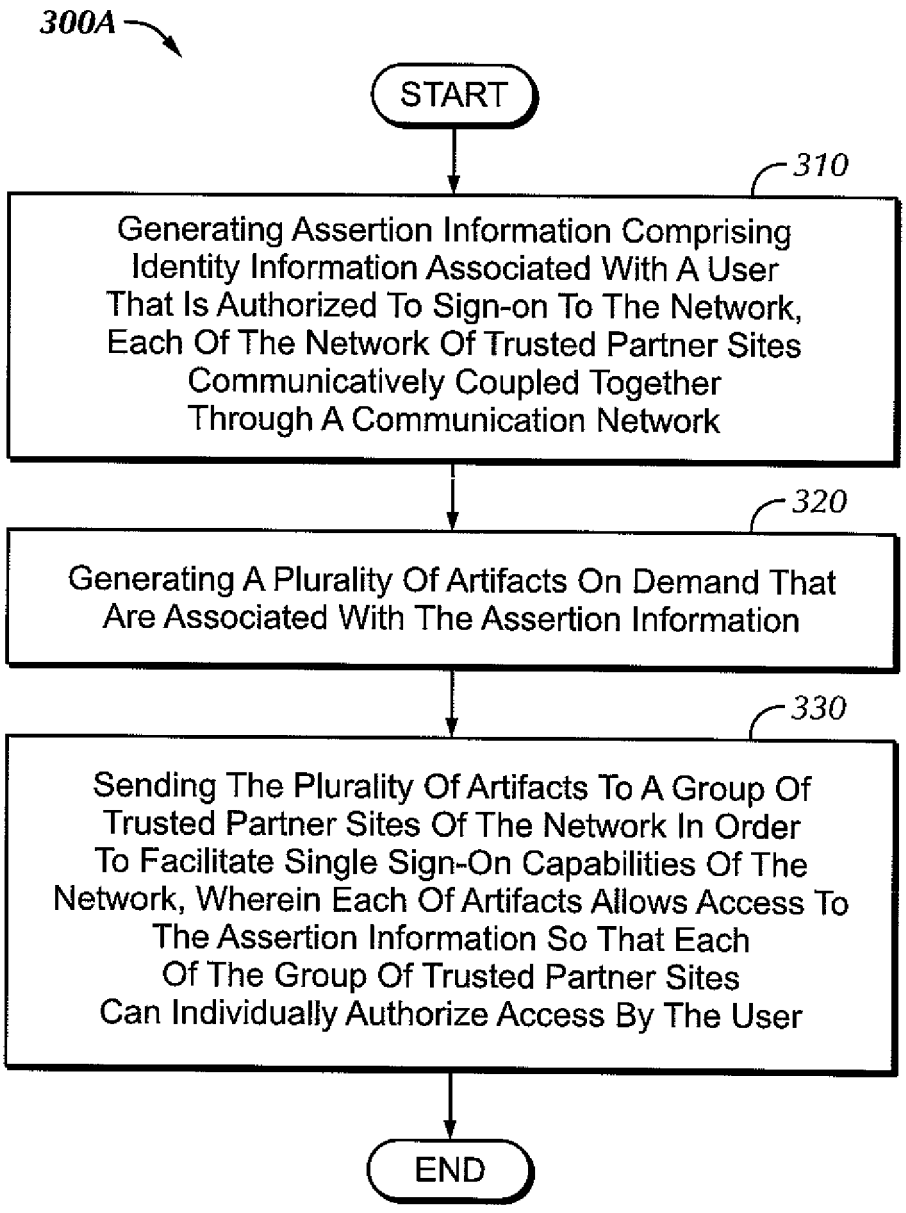
300A
START
310
Generating Assertion Information Comprising Identity Information Associated With A User That Is Authorized To Sign-on To The Network, Each Of The Network Of Trusted Partner Sites Communicatively Coupled Together Through A Communication Network
320
Generating A Plurality Of Artifacts On Demand That Are Associated With The Assertion Information
330
Sending The Plurality Of Artifacts To A Group Of Trusted Partner Sites Of The Network In Order To Facilitate Single Sign-On Capabilities Of The Network, Wherein Each Of Artifacts Allows Access To The Assertion Information So That Each Of The Group Of Trusted Partner Sites Can Individually Authorize Access By The User
END

FIG. 3A

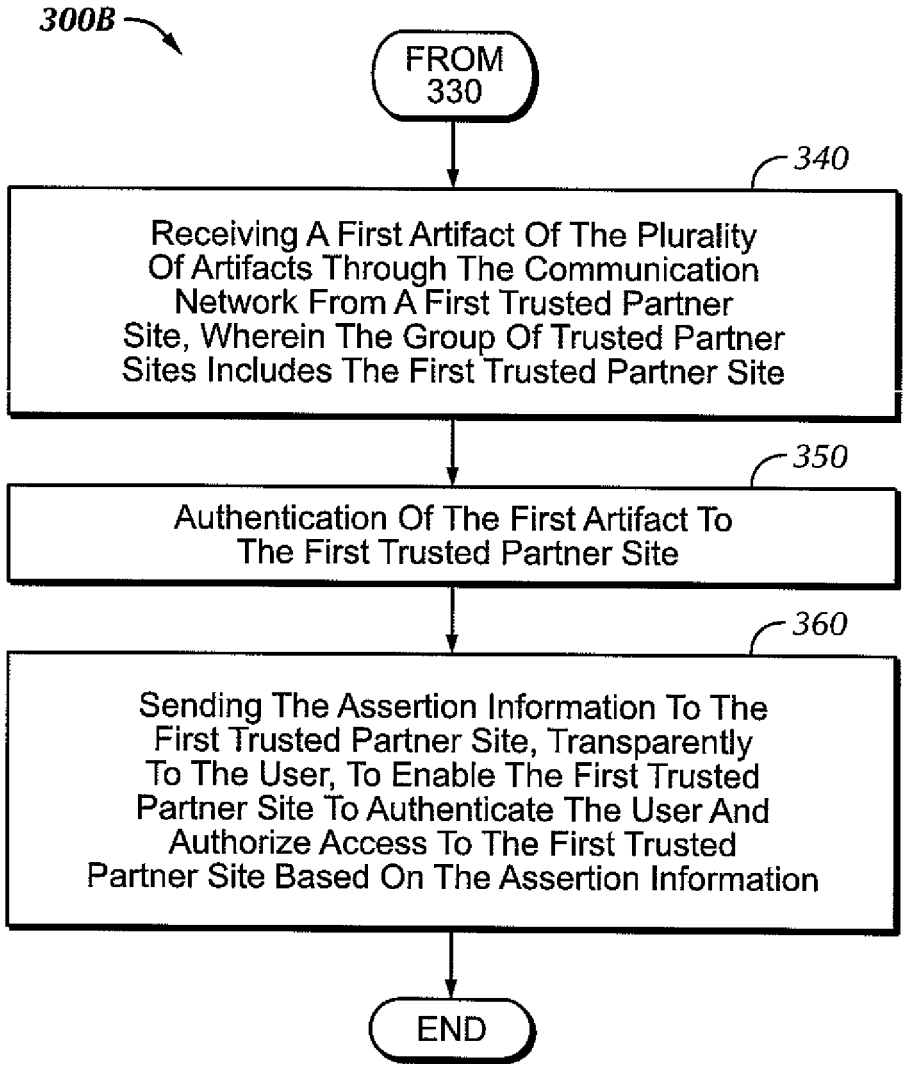
300B
FROM 330
340
Receiving A First Artifact Of The Plurality Of Artifacts Through The Communication Network From A First Trusted Partner Site, Wherein The Group Of Trusted Partner Sites Includes The First Trusted Partner Site
350
Authentication Of The First Artifact To The First Trusted Partner Site
360
Sending The Assertion Information To The First Trusted Partner Site, Transparently To The User, To Enable The First Trusted Partner Site To Authenticate The User And Authorize Access To The First Trusted Partner Site Based On The Assertion Information
END

FIG. 3B

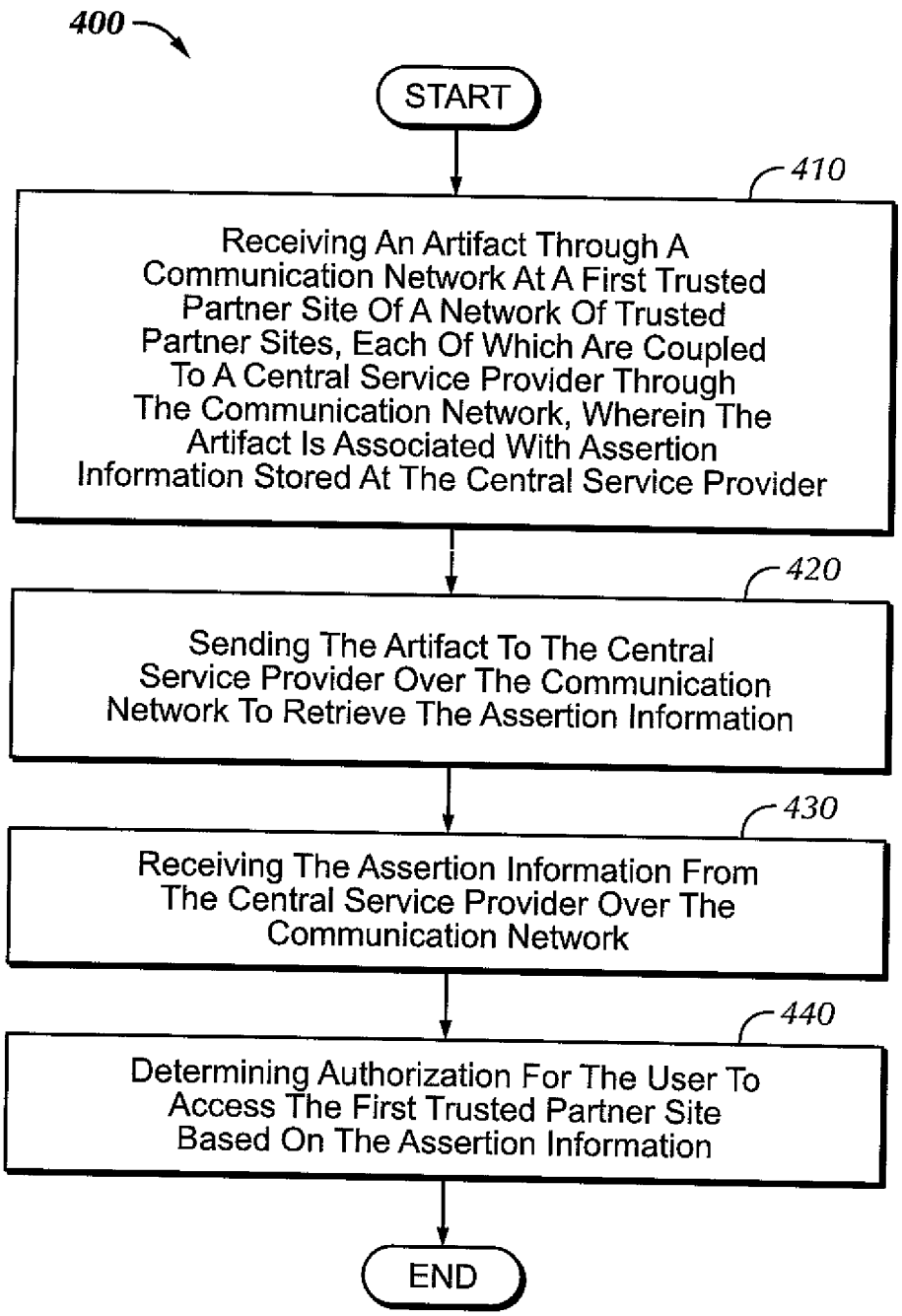
400
START
410
Receiving An Artifact Through A Communication Network At A First Trusted Partner Site Of A Network Of Trusted Partner Sites, Each Of Which Are Coupled To A Central Service Provider Through The Communication Network, Wherein The Artifact Is Associated With Assertion Information Stored At The Central Service Provider
420
Sending The Artifact To The Central Service Provider Over The Communication Network To Retrieve The Assertion Information
430
Receiving The Assertion Information From The Central Service Provider Over The Communication Network
440
Determining Authorization For The User To Access The First Trusted Partner Site Based On The Assertion Information
END

FIG. 4

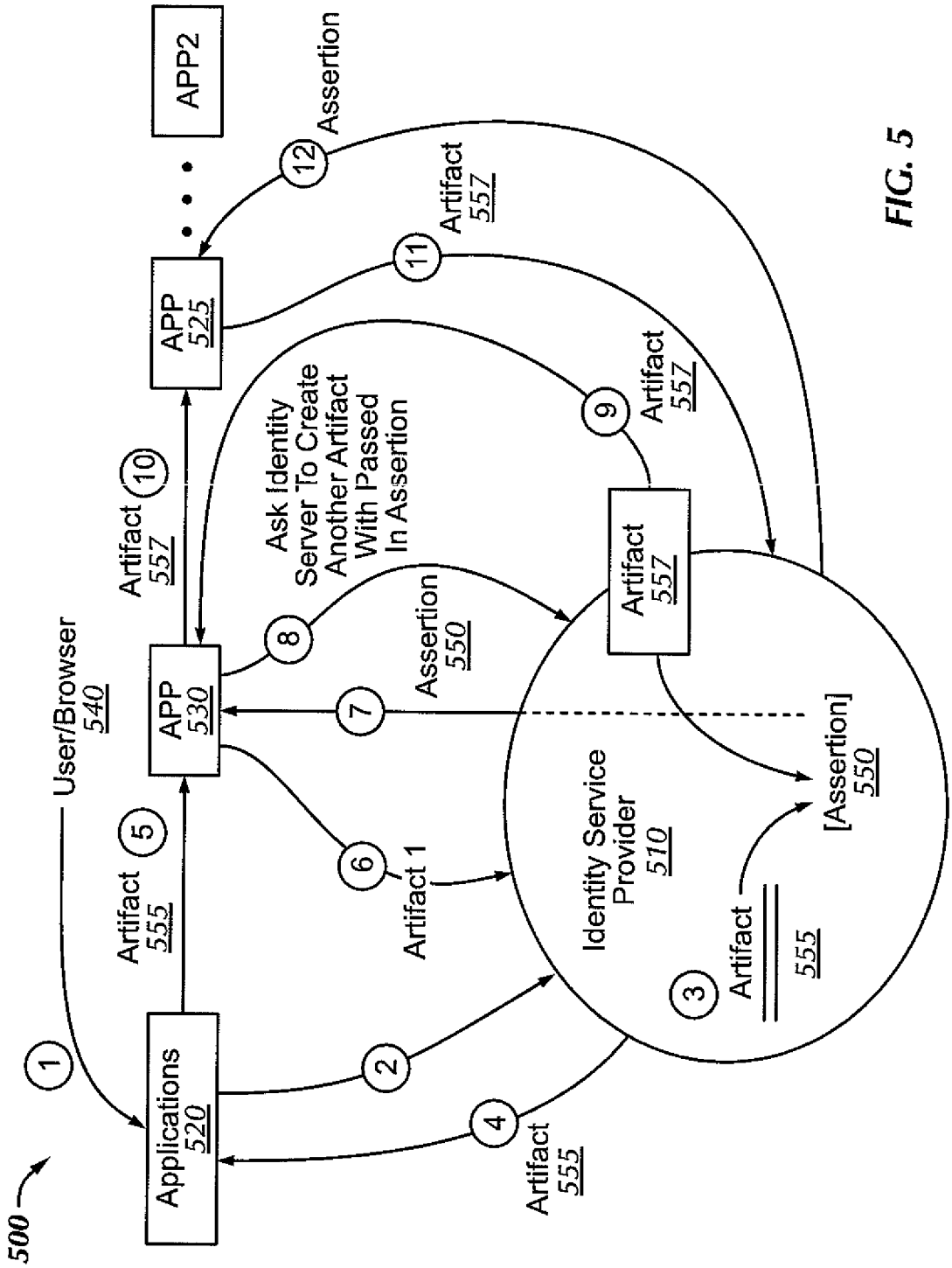
500
Applications 520
User/Browser 540
APP 530
APP 525
APP2
Identity Service Provider 510
Artifact 555
Artifact 1
Artifact 555
Assertion 550
Ask Identity Server To Create Another Artifact With Passed In Assertion
Artifact 557
Artifact 557
Artifact 557
Artifact 557
Assertion
[Assertion] 550
1
2
3
4
5
6
7
8
9
10
11
12

FIG. 5

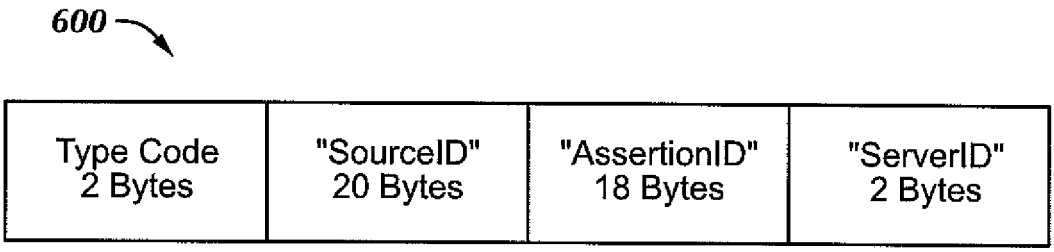
600
Type Code
2 Bytes
"SourceID"
20 Bytes
"AssertionID"
18 Bytes
"ServerID"
2 Bytes

FIG. 6

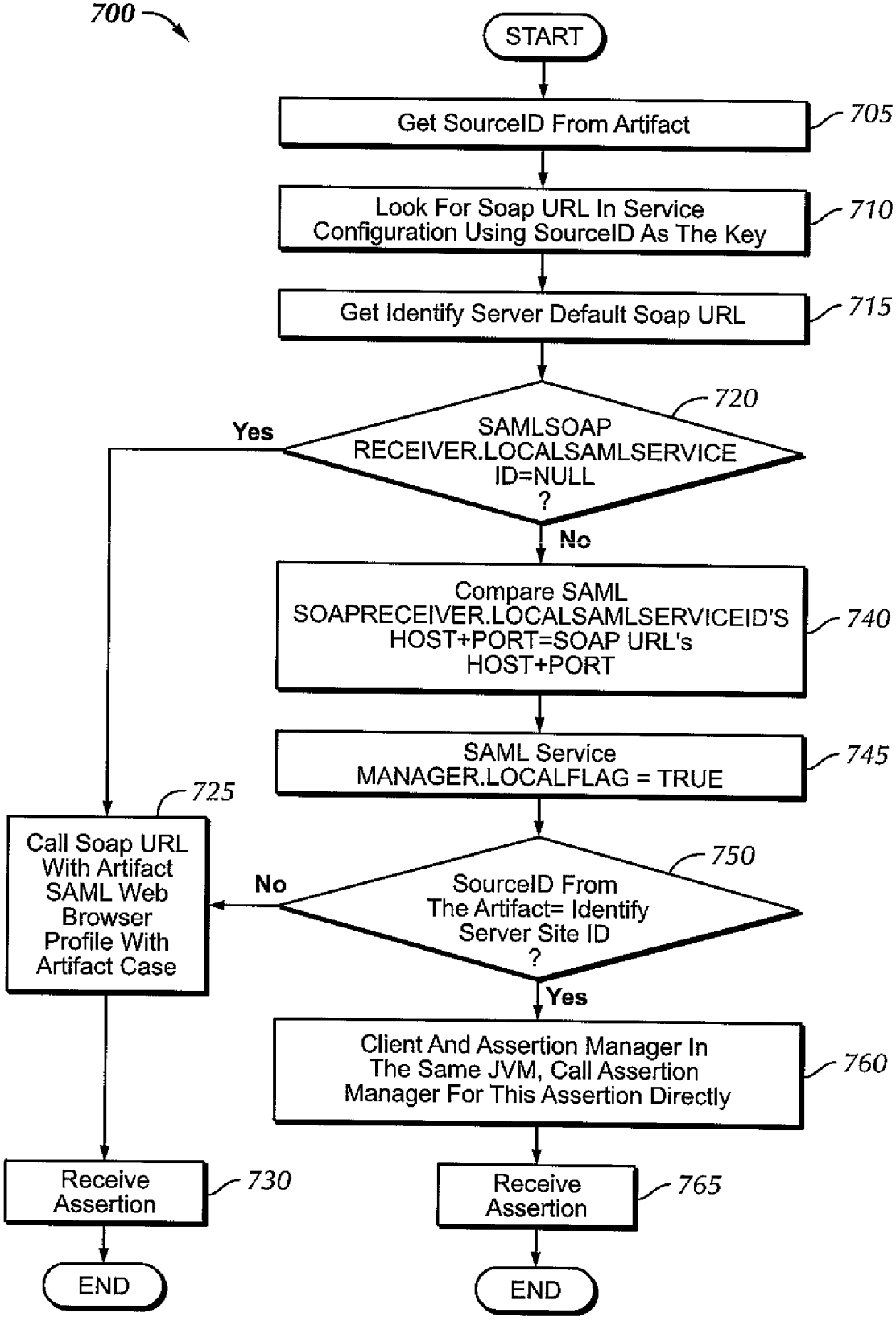
700
START
Get SourceID From Artifact
705
Look For Soap URL In Service Configuration Using SourceID As The Key
710
Get Identify Server Default Soap URL
715
720
SAMLSOAP RECEIVER.LOCALSAMLSERVICE ID=NULL ?
Yes
No
Compare SAML SOAPRECEIVER.LOCALSAMLSERVICEID'S HOST+PORT=SOAP URL's HOST+PORT
740
SAML Service MANAGER.LOCALFLAG = TRUE
745
725
Call Soap URL With Artifact SAML Web Browser Profile With Artifact Case
750
SourceID From The Artifact= Identify Server Site ID ?
No
Yes
Client And Assertion Manager In The Same JVM, Call Assertion Manager For This Assertion Directly
760
Receive Assertion
730
Receive Assertion
765
END
END

FIG. 7